UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,752	10/31/2001	Richard H. Harris	RPS920010068US1	3546

7590 06/17/2004

SAWYER LAW GROUP
P.O. Box 51418
Palo Alto, CA 94303

EXAMINER	
AU, SCOTT D	
ART UNIT	PAPER NUMBER
2635	4

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/002,752	**Applicant(s)** HARRIS, RICHARD H.	
	Examiner Scott Au	**Art Unit** 2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 4/5/04.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-16 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to applicant's response to an Amendment A, which is filed April 5, 2004.

An amendment A to the claims 1-16 have been entered and made of record in the Application of Harris for an "Secure smart card" filed October 31, 2001.

Claims 1-16 are pending.

Response to Arguments

Applicant's amendments and argument with respected to the pending claims 1-16, filed April 5, 2004, have been fully considered but they are not persuasive for at least the following reasons.

On page 9, third paragraph, Applicant's argument with respect to the invention that Application's specification defines "the identification verification data is for the purpose of activating the transaction device, not for the facilitation of the secure transaction", is not persuasive.

Lessin et al. disclose that the cardholder operates the ITC through a plurality of menus. The menus present to the cardholder the options that are available to the cardholder at that specific point in the program. The options presented may be sub-menus of the menu currently being displayed or the options presented may be a selection of variables to be used during the execution of an application program. For example, the cardholder may select a menu item identified by "CREDIT" to activate a credit function. A sub-menu of credit options, such as making a credit transaction or seeing the cardholder's credit balance, is then presented to the cardholder. Once the cardholder selects an application the cardholder is prompted to enter variables used in the application (col. 10 lines 41-54).

On page 9, third paragraph, Applicant's argument with respect to the invention that Application's specification defines "when the input of the identification verification data is received, the transaction device is in a deactivated state", is not persuasive.

Lessin et al. disclose that the cardholder is prompted by display 25 to enter in his PIN by the prompt depicted in box 762. The entered PIN is then tested at step 764 against a PIN that is stored in the ITC in conjunction with this application program. This prevents unauthorized access to this application program because the cardholder should be the only person who knows his PIN. If an incorrect PIN is entered, system control exits the application program and returns to the point in the program that generates the display shown in box 754. If the cardholder enters the correct PIN, the system displays on display 25 the first note stored in memory as shown in box 766, indicating to the cardholder that he now can access his notes (col. 11 lines 46-58). Examiner interprets the Intelligent Transaction Card is not activated and remain in the deactivation mode when the PIN is entered and is in activation mode only when the correct PIN is read.

On page 10, Applicant's argument with respect to the pending claims 9-10 and 12-14 filed April 5, 2004, is persuasive. Therefore the examiner has withdrawn the rejections.

On page 12, fourth paragraph, Applicant's argument with respect to the invention that Application's specification defines "Applicant disagrees that one of ordinary skill in the art at the time the invention was made would be motivated to combine Lessin and Grant", is not persuasive.

In response to Applicant's argument that there is no suggestion to combine the references, the Examiner recognizes that reference cannot be arbitrarily combined and that there must be some reason why one skilled in the art would be motivated to make the proposed combination of primary and secondary references. *In re Nomiya*, 184 USPQ 607 (CCPA 1975). However, there in no requirement that a motivation to make the modification be expressly articulated. The test for combining references is what the combination of disclosures taken as a whole would suggest to one of ordinary skill in the art. *In re McLaughlin*, 170 USPQ 209 (CCPA 1971).

Lessin et al. disclose a method the cardholder selects the change PIN function, the cardholder is prompted to enter the current PIN by the display depicted in box 860. The entered PIN is then tested at step 862 against the PIN already stored in the ITC. If the PIN is incorrect, i.e. it does not match the PIN stored in the system, the system gives the cardholder another opportunity to enter the PIN by generating the display shown. The PIN that is entered is tested at step 866. If the correct PIN is entered, the cardholder is prompted for the new PIN he wishes to enter by displays 868 and 870. After the new PIN is entered at step 872, the cardholder is prompted to reenter the new PIN by displays 874, 876. At step 878, the two new PINS are compared. If the PIN entered in response to the display at box 876 does not match the PIN entered in response to the display at box 870, an error message is displayed as shown at box 880 and the cardholder is given another opportunity to enter the correct PIN by returning the program to the point at which the display shown in box 870 is generated. If the cardholder fails to enter in the correct PIN after a predetermined number of tries, the new PIN does not replace the current PIN and the system returns to the point that generates the display of box 860 where the cardholder has to again enter the current PIN. If, at step 878, the cardholder re-enters the new PIN correctly, the current PIN is replaced with the new PIN and the cardholder is informed of this by the display at box 884. The application is then exited (col. 13 lines 20-48; see Figure 15C).

In the same field of endeavor of method and device for preventing unauthorized use of credit cards, Grant et al. disclose a method that once the correct PIN code is entered, the card is activated for a predetermined limited time. After the predetermined time, the card returns to the disable state so that it cannot be used for a fraudulent transaction (col. 3 lines 59-62).

One of ordinary skill in the art understands that timer of Grant et al. is desirable in Intelligent Transaction Card device of Lessin et al. because Lessin et al. suggest the communication service routine executes the proper data handshaking with the proper timing, reads in the data transmitted to the data port and stores it in a memory buffer.

Since the only information that is presented to a communication port relates to a specific application, the application service routine is initiated at step 317 after the information is received from the port (col. 5 lines 61-68) and Grant et al. teach once the correct PIN code is entered, the card is activated for a predetermined limited time. After the predetermined time, the card returns to the disable state so that it cannot be used for a fraudulent transaction. The means for putting the card in the enable state are preferably contained within the card, such as being entered into a small keypad built into the card. However, the means for placing the card in the enable state may be located at a portable auxiliary device, or through other suitable means (col. 3 lines 58-67). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include a timer of Grant et al. in the Intelligent transaction card device of Lessin et al. with the motivation for doing so would allow a predetermined of time is set for the user to enter the correct PIN before the time expired.

On page 13, fourth paragraph, Applicant's argument with respect to the invention that Application's specification defines "Lessin et al. in view of Hewig does not teach or suggest the elements as recited in the combination of claims 1 and 5", is not persuasive.

In response to Applicant's argument that there is no suggestion to combine the references, the Examiner recognizes that reference cannot be arbitrarily combined and that there must be some reason why one skilled in the art would be motivated to make the proposed combination of primary and secondary references. *In re Nomiya*, 184 USPQ 607 (CCPA 1975). However, there in no requirement that a motivation to make the modification be expressly articulated. The test for combining references is what the combination of disclosures taken as a whole would suggest to one of ordinary skill in the art. *In re McLaughlin*, 170 USPQ 209 (CCPA 1971).

Lessin et al. disclose the method that the cardholder operates the ITC through a plurality of menus. The menus present to the cardholder the options that are available to the cardholder at that specific point in the program. The options presented may be sub-menus of the menu currently being displayed or the options presented may be a selection of variables to be used during the execution of an application program. For example, the cardholder may select a menu item identified by "CREDIT" to activate a credit function. A sub-menu of credit options, such as making a credit transaction or seeing the cardholder's credit balance, is then presented to the cardholder (col. 10 lines 41-52).

In the same field of endeavor of method and apparatus for utilizing a smart card, Herwig discloses deactivating the transaction device when the secure transaction is completed (page. 4 paragraph 38) in order to have a secured retail transaction account.

One of ordinary skill in the art understands that deactivating the transaction device when the transaction is completed is desirable in the Intelligent transaction card device of Lessin et al. because Lessin et al. suggest The ITC may also be used to independently authorize a credit transaction and generate an approval code thus eliminating the need to use a bank terminal (col. 3 lines 50-55) and Hewig teaches a hand-held computing device 14, completed a retail transaction or inquiry, and therefore deactivated the retail the device (page 4, paragraph 38). Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include step: deactivating the transaction device when the secure transaction is completed of method and apparatus for utilizing a smart card disclosed by Herwig into portable interactive personal data system of Lessin et al. with the motivation for doing so would allow the transaction device to deactivate after a transaction is completed.

On page 13, sixth paragraph, Applicant's argument with respect to the invention that Application's specification defines "Lessin et al. in view of Grant et al. and further in view of Herwig still does not teach or suggest the elements as recited in the combination of claims of steps as recited in amended independent claim 8", is not persuasive.

In response to Applicant's argument that there is no suggestion to combine the references, the Examiner recognizes that reference cannot be arbitrarily combined and that there must be some reason why one skilled in the art would be motivated to make the proposed combination of primary and secondary references. *In re Nomiya*, 184 USPQ 607 (CCPA 1975). However, there in no requirement that a motivation to make the modification be expressly articulated. The test for combining references is what the combination of disclosures taken as a whole would suggest to one of ordinary skill in the art. *In re McLaughlin*, 170 USPQ 209 (CCPA 1971).

Referring to claim 8, Lessin et al. in view of Grant et al. and Herwig disclose a method of claims 5 and 7, claim 8 equivalent to that the combine of claim 5 and claim 7 "steps a-g" addressed above, incorporated herein. Therefore, claim 8 is rejected for the same reasons given with respect to claims 5 and 7 "steps a-g" combined.

On page 14, Applicant's argument with respect to the pending claim 11 filed April 5, 2004, is persuasive. Therefore the examiner has withdrawn the rejections.

On page 15, Applicant's argument with respect to the pending claim 15-16 filed April 5, 2004, is persuasive. Therefore the examiner has withdrawn the rejections.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2 and 6 are rejected under 35 U.S.C. 102(b) as being anticipated by Lessin et al. (US# 4,868,376).

Referring to claim 1, Lessin et al. disclose a method for providing a secure transaction, comprising the steps of:

(a) receiving a new identification (i.e. new PIN) verification data by a transaction device(10) (i.e. a programmable intelligent transaction card (ITC)) directly from a user;

(b) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device (col. 3 lines 7-27 and col. 13 lines 20-48; see Figures 1A and 15C);

(c) receiving an input of an identification verification data by the transaction device directly from the user, wherein the transaction device is in a deactivated state (col. 5 lines 15-24 and col. 11 lines 48-58);

(d) activating the transaction device if the inputted identification verification data matches the new identification verification data (col. 5 lines 14-24); and

(e) deactivating the transaction device when an event occurs (i.e. routine exited) (col. 8 lines 27-38).

Referring to claim 2, Lessin et al. disclose the method of claim 1, wherein the receiving step (a) comprises:

(al) assigning an initial identification verification data to the user (i.e. current PIN of the user);

(a2) receiving the initial identification verification data by the transaction device directly from the user (i.e. step 860);

(a3) verifying the initial identification verification data by the transaction device (i.e. step 862);

(a4) receiving an indication of a new identification verification data by the transaction device (i.e. step 872); and

(a5) receiving the new identification verification data by the transaction device directly from the user (i.e. step 878) (col. 13 lines 20-48; see Figure 15C).

Referring to claim 6, Lessin et al. disclose the method of claim 1 wherein the new identification verification data comprises at least one of the following:

a personal identification number ;a fingerprint; or a signature (col. 4 lines 7-11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9-10 and 12-14 are rejected under 35 U.S.C 103(a) as being unpatentable over Nara et al. (US# 4,766,294) in view of Mears (US# 5,539,400).

Referring to claim 9, Nara et al. disclose a transaction device, comprising:

an inputting means (12) (i.e. keyboard) for receiving an inputted identification verification data (col. 2 lines 41-55; see Figure 3);

a decoder (i.e. CPU able to do the decoding process), wherein the inputted identification verification data is not shared with another device; and a processor (28) (i.e. CPU) coupled to the decoder (i.e. CPU acts as processor and decoder), wherein the decoder asserts an activation signal to the processor (28) (i.e. CPU) if the identification verification data is verified, wherein the decoder de-asserts the activation signal when an event occurs and wherein the inputted identification verification data is not shared with another device (col. 2 lines 26-34, col. 3 lines 18-58, col. 9 lines 59-61 and col. 11 lines 25-30, 57-60).

In the same field of endeavor of decoding device, Mears discloses a decoder (90) (i.e. an encoder logic) coupled to the inputting means (52) (i.e. keypad array) for sensing, decoding, and verifying the inputted identification verification data (col. 4 lines 9-19; see Figures 1-2 and 4) in order to analyze the keypad array input logic when one of the sensor circuit detect a depressed key.

One of ordinary skill in the art understands that decoder of Mears is desirable in the portable medium of Nara et al. because Nara et al. suggest CPU 28 for control the circuit operations. Program ROM 29 for storing control programs, memory 30 for program working, and data memory 31, made up of a PROM, for storing a personal identification number of four digits, for example, and data are further included. The IC circuit further includes timer 32 for time counting during the data processing (col. 3 lines 29-36) and Mears teaches sensor circuit s 93A-93D detects keypad array (54) communicate with microcontroller (56) when keys are depressed (col. 4 lines 16-20). Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include an encoder logic coupled to the keypad array for sensing, detecting and verifying a depressed key disclosed by Mears between the input control and a CPU of Nara et al. with the motivation for doing so would allow faster for the CPU to process and more reliable in order to improve transaction device operate efficiently.

Referring to claim 10, Nara et al. in view of Mears disclose the device of claim 9, Nara et al. disclose wherein the event comprises a completion of a secure transaction (col. 3 lines 19-59).

Referring to claim 12, Nara et al. in view of Mears disclose the device of claim 9, Mears discloses wherein the inputting means comprises a plurality of capacitive keys, wherein each capacitive key comprises a first side and a second side (col. 3 lines 17-29; see Figures 2 and4) where is coupled to oscillator on one side and coupled to the decoder (90) (i.e. encoder function as decoder) on the second side.

Referring to claim 13, Nara et al. in view of Mears disclose the device of claim 9, Mears discloses further comprising: an oscillator (70) (i.e. an oscillator) coupled to the inputting means (52) (i.e. keypad array); and a power source (62) (i.e. battery) coupled to the oscillator (70) (i.e. an oscillator) and the decoder (90) (i.e. an encoder functions as decoder) (col. 3 lines 17-29 and col. 4 lines 9-19; see Figure 1-2 and 4).

Referring to claim 14, Nara et al. view of Mears disclose the device of claim 9, Nara et al. disclose wherein the decoder (i.e. CPU also function as a decoder that can verify the data, stored data in memory and determining identification data matches) comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data (col. 2 lines 26-34, col. 3 lines 18-59, col. 9 lines 59-61 and col. 11 lines 25-30, 57-60).

Claims 3-4 and 7 are rejected under 35 U.S.C 103(a) as being unpatentable over Lessin et al. (US# 4,868,376) in view of Grant et al. (US# 6,095,416).

Referring to claim 3, Lessin et al. disclose the method of claim 1, wherein the activating step (d) comprises:

(dl) determining if the inputted identification verification data matches the new identification verification data by the transaction device (i.e. step 124);

(d2) activating the transaction device if the inputted identification verification data matches the new identification verification data (i.e. step 128) (col. 5 lines 15-24; see Figure 4). However, Lessin et al. did not explicitly disclose step:

(d3) starting a timer if the transaction device is activated, wherein the timer expires after the predetermined period of time.

In the same field of endeavor of method and device for preventing unauthorized use of credit cards, Grant et al. disclose step: starting a timer if the transaction device is activated, wherein the timer expires after the predetermined period of time (col. 3 lines 59-62) in order to disable the transaction after a predetermined limited of time to prevent a fraudulent transaction.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include step: starting a timer if the transaction device is activated, wherein the timer expires after the predetermined period of time of credit cards method and system disclosed by Grant et al. into portable interactive personal data system of Lessin et al. with the motivation for doing so would allow the transaction to deactivate after a predetermined limited of time to prevent fraudulent transaction.

Referring claim 4, Grant et al. disclose the method of claim 3, wherein the deactivating step (e) comprises:

(e1) deactivating the transaction device when the timer expires (col. 3 lines 59-62).

Referring claim 7, Lessin et al. disclose a method for providing a secure transaction, comprising the steps of:

(a) receiving an initial identification verification data by the transaction device directly from the user (i.e. step 860);

(b) verifying the initial identification verification data by the transaction device (i.e. step 862);

(c) receiving a new identification verification data by the transaction device directly from the user (i.e. step 878) (col. 13 lines 20-48; see Figure 15C);

(d) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device (col. 3 lines 7-27 and col. 13 lines 20-48; see Figures 1A and 15C);

(e) receiving an input of an identification verification data by the transaction device directly from the user, wherein the transaction device is in a deactivated state (col. 5 lines 15-24 and col. 11 lines 48-58);

(f) determining if the inputted identification verification data matches the new identification verification data by the transaction device (col. 5 lines 15-24);

(g) activating the transaction device if the inputted identification verification data matches the new identification verification data (col. 5 lines 15-24).

However, Lessin et al. did not explicitly disclose step:

(h) starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and

(i) deactivating the transaction device when the timer expires.

In the same field of endeavor of method and device for preventing unauthorized use of credit cards, Grant et al. disclose steps:

(h) starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and

(i) deactivating the transaction device when the timer expires (col. 3 lines 59-62) in order to disable the transaction after a predetermined limited of time so that it cannot be used for a fraudulent transaction.

One of ordinary skill in the art understands that timer of Grant et al. is desirable in Intelligent transaction card device of Lessin et al. because Lessin et al. suggest the communication service routine executes the proper data handshaking with the proper timing, reads in the data transmitted to the data port and stores it in a memory buffer. Since the only information that is presented to a communication port relates to a specific application, the application service routine is initiated at step 317 after the information is received from the port (col. 5 lines 61-68) and Grant et al. teach once the correct PIN code is entered, the card is activated for a predetermined limited time. After the predetermined time, the card returns to the disable state so that it cannot be used for a fraudulent transaction. The means for putting the card in the enable state are preferably contained within the card, such as being entered into a small keypad built into the card. However, the means for placing the card in the enable state may be located at a portable auxiliary device, or through other suitable means (col. 3 lines 58-67). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include a timer of Grant et al. in the Intelligent transaction card device of Lessin et al. with the motivation for doing so would allow a predetermined of time is set for the user to enter the correct PIN before the time expired.

Claim 5 is rejected under 35 U.S.C 103(a) as being unpatentable over Lessin et al. (US# 4,868,376) in view of Herwig (US# 2002/0082925).

Referring to claim 5, Lessin et al. disclose the method of claim 1. However, Lessin et al. did not explicitly disclose wherein the deactivating step (e) comprises:

(el) deactivating the transaction device when the secure transaction is completed.

In the same field of endeavor of method and apparatus for utilizing a smart card, Herwig discloses deactivating the transaction device when the secure transaction is completed (page. 4 paragraph 38) in order to have a secured retail transaction account. One of ordinary skill in the art understands that deactivating the transaction device when the transaction is completed is desirable in the Intelligent transaction card device of Lessin et al. because Lessin et al. suggest The ITC may also be used to independently authorize a credit transaction and generate an approval code thus eliminating the need to use a bank terminal (col. 3 lines 50-55) and Hewig teaches a hand-held computing device 14, completed a retail transaction or inquiry, and therefore deactivated the retail the device (page 4, paragraph 38). Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include step: deactivating the transaction device when the secure transaction is completed of method and apparatus for utilizing a smart card disclosed by Herwig into portable interactive personal data system of Lessin et al. with the motivation for doing so would allow the transaction device to deactivate after a transaction is completed.

Claim 8 is rejected under 35 U.S.C 103(a) as being unpatentable over Lessin et al. (US# 4,868,376) in view of Herwig (US# 2002/0082925).

Referring to claim 8, Lessin et al. in view of Grant et al. and Herwig disclose a method of claims 5 and 7, claim 8 equivalent to that the combine of claim 5 and claim 7 "steps a-g" addressed above, incorporated herein. Therefore, claim 8 is rejected for the same reasons given with respect to claims 5 and 7 "steps a-g" combined.

Claim 11 is rejected under 35 U.S.C 103(a) as being unpatentable over Nara et al. (US# 4,766,294) in view of Mears (US# 5,539,400) and further in view of Grant et al. (US# 6,095,416).

Referring to claim 11, Nara et al. in view of Mears disclose the device of claim 9. Nara et al. disclose a timer circuit (32) (i.e. timer) coupled to the decoder (i.e. part of a CPU). However, Nara et al. in view of Mears did not explicitly disclose wherein the timer circuit is initiated when the decoder asserts the activation signals, wherein the timer circuit expires after a predetermined period of time, wherein the event comprise the expiration circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

In the same field of endeavor of authorization of card, Grant et al. disclose wherein the timer circuit (col. 4 line 57) is initiated when the decoder (col. 8 lines 54-55) asserts the activation signals, wherein the timer circuit (col. 4 line 57) expires after a predetermined period of time, wherein the event comprise the expiration circuit, wherein the decoder (col. 8 lines 54-55) de-asserts the activation signal to the processor when the timer circuit expires (col. 3 lines 59-62) to prevent fraudulent transaction.

One of ordinary skill in the art understands that the security method of activating signals for a predetermined time of Grant et al. is desirable in transaction device of Nara et al. in view of Mears becauser Nara et al. suggest an IC card, as a portable medium, has an oscillator for generating a low-frequency clock signal for time-piece. A display clock for display is provided for counting the clock signal. The time based on a count carried out by the display clock is displayed on the IC card a display section. In this case, the count of the display clock can be changed, as appropriate, by using keys on the keyboard provided on the IC card. The IC card also incorporates a transaction clock for counting the clock signal (i.e. see abstract). Further more, Nara et al. disclose the IC card can be used independently, and a stand-by mode in which the IC cards counts time alone (col. 2 lines 30-34). Mears teaches sensor circuit s 93A-93D detects keypad array (54) communicate with microcontroller (56) when keys are depressed (col. 4 lines 16-20). Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include the signal activation method of Grant et al. in the transaction device of Nara et al. in view of Mears with the motivation for doing so would allow the device is secured after activating for a predetermined of time.

Claim 15 is rejected under 35 U.S.C 103(a) as being unpatentable over Mears (US# 5,539,400) in view of Wallerstein (US# 5,585,787) and further in view of Grant et al. (US# 6,095,416).

Referring to claim 15, Mears discloses a transaction device (50) (i.e. system of transaction device), comprising:

a plurality of capacitive keys for inputting an identification verification data, wherein each capacitive key comprises a first side and a second side (col. 3 lines 17-29; see Figures 2 and 4); an oscillator coupled to the first side of each capacitive key; a power source (62) (i.e. battery) coupled to the oscillator(70) (i.e. an oscillator) and the decoder (90) (i.e. an encoder functions as a decoder) (col. 3 lines 17-29 and col. 4 lines 9-19; see Figures 1-2 and 4).

However, Mears did not explicitly disclose a decoder coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled, wherein the decoder comprises a stored identification verification data, wherein the stored identification verification data is not shared with another device, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data; a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified; and a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

In the same field of endeavor of programmable credit card system, Wallerstein discloses a decoder (40) (i.e. CPU able to do the decoding process) coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled, wherein the decoder (40) (i.e. CPU able to do the decoding process) comprises a stored identification verification data, wherein the stored identification data is not shared with another device (col. 2 lines 18-24, referring to Hara et al. disclose that IC card identification information is not shared with another device), wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data; a processor coupled to the decoder (i.e. CPU also works as a decoder), wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified (col. 6 lines 9-28; see Figure 4) in order to have a secured transaction.

One of ordinary skill in the art understands that CPU (40) works as a decoder and control the ROM 43 and RAM44 with in the "Background of the invention", (col. 2 lines 18-23, referring to Hara et al. disclose a IC card that identification information is not shared with another device) is desirable in the keypad encode method of Mears because Mears teaches sensor circuit s 93A-93D detects keypad array (54) communicate with microcontroller (56) when keys are depressed (col. 4 lines 16-20). Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include a decoder coupled to the second side of each capacitive key for sensing, decoding, and verifying the inputted identification verification data when the first and second sides of at least one of the capacitive keys are coupled, wherein the decoder comprises a stored identification verification data, wherein the decoder verifies the inputted identification verification data by determining that the inputted identification verification data matches the stored identification verification data; a processor coupled to the decoder, wherein the decoder asserts an activation signal to the processor if the inputted identification verification data is verified of programmable credit card system disclosed by Wallerstein into keypad encoder of a device of Mears with the motivation for doing so would allow data is verified, sensed , decoded and stored when the transaction is processed.

However, Mears in view of Wallerstein did not explicitly disclose a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires.

In the same field of endeavor of IC card identification system, Grant et al. teach a timer circuit (col. 4 line 57) coupled to the decoder (col. 8 lines 54-55), wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor (col. 3 lines 59-63) in order to prevent fraudulent transaction.

One of ordinary skill in the art understands that the security method of activating signals for a predetermined time of Grant et al. is desirable in the transaction device of Mears in view of Wallerstein because Grant et al. disclose that once the correct PIN code is entered, the card is activated for a predetermined limited time. After the predetermined time, the card returns to the disable state. Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires of IC card identification system of Grant et al. in transaction system of Mears in view of Wallerstein with the motivation for doing so would allow the transaction to deactivate after a predetermined limited of time to prevent fraudulent transaction.

Claim 16 is rejected under 35 U.S.C 103(a) as being unpatentable over Mears (US# 5,539,400) in view of Wallerstein (US# 5,585,787), Grant et al. (US# 6,095,416) of the extent of claim 15 above.

Referring to claim 16, Wallerstein discloses the decoder de-asserts the activation signal to the process when a secure transaction is completed (col. 6 lines 9-28 and col. 7 lines 27-37; see Figure 5). Therefore, one skilled in the art understand that the (40) CPU of Wallerstein functions as a processor and a decoder where signal is de-asserted to the CPU when a secure transaction is completed.

Conclusion

Any inquiry concerning this communication or earlier communications form the examiner should be directed to Scott Au whose telephone number is (703) 305-4680. The examiner can normally be reached on Mon-Fri, 8:30AM – 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached at (703) 305-4704. The fax phone numbers for the organization where this application or proceeding is assigned are (703)-872-3906.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)-305-3900.

Scott Au

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600